UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

United Resource Systems, Inc., Plaintiff, v. The State of South Carolina by and through Alan Wilson, in his official capacity as Attorney General of South Carolina, Defendant.	Case No.: 3:21-364-JFA **COMPLAINT** **(non-jury trial)**

I. NATURE OF THE ACTION

1. On May 18, 2018, Governor Henry McMaster signed into law H.4628, the "South Carolina Telephone Privacy Protection Act" (the "Act"). The Act became effective when signed.

2. The Act amended the Code of Laws of South Carolina, 1976, by adding a new chapter, Chapter 21, to Title 37, which is more commonly known as the Consumer Protection Code.

3. The Act includes S.C. Code Ann. § 37-21-50 (2018), titled "Accuracy of caller identification information required; exceptions" (the "Anti-Spoofing Provision"), which states, in relevant part:

> (A) Notwithstanding another provision of law, a person may not, with the intent to defraud, harass, cause harm or wrongfully obtain anything of value, including, but not limited to, financial resources or personal identifying information as defined in Section 16-13-510, make, place, or initiate a call or text message or engage in conduct that results in the display of misleading, false or inaccurate caller identification information on the receiving party's telephone or otherwise circumvent caller identification technology that allows the receiving party to identify from what phone number, location, or organization the call or text message has originated from or misrepresent the origin and nature of the call or text message. A person may not, with the intent described in this subsection:

> (1) display a South Carolina area code on the recipient's caller identification system unless the person making, placing, or initiating the call or text message maintains a physical presence in the State; or
>
> (2) display the receiving party's telephone number on the contacted party's caller identification system.

4. A person found to have violated the Anti-Spoofing Provision of the Act is subject to potentially substantial civil liability. For actions brought by a call recipient, in addition to actual losses and attorney's fees, the call recipient can recover statutory damages between $1,000 and $5,000 for ***each violation.*** S.C. Code Ann. § 37-21-80(A) – (C) (2018). The Attorney General is also charged with investigating and enforcing violations of the Act and can bring an action on behalf of one or more call recipients in which he is permitted to "recover damages for an aggrieved person or persons in the amount of five thousand dollars for each violation…" and "a civil penalty of not more than five thousand dollars for each violation…" "[i]f the court finds a willful violation…" S.C. Code Ann. § 37-21-90(B)(1) – (2) (2018).

5. Plaintiff brings this action under 28 U.S.C. §§ 2201 and 2202 seeking a declaration that the Anti-Spoofing Provision is in conflict with, and therefore preempted by, the federal Truth in Caller ID Act of 2009, Public Law 111-331, 47 U.S.C. § 227(e), and that the Anti-Spoofing Provision is unconstitutional, both on its face and as applied to Plaintiff. Plaintiff seeks a permanent injunction preventing enforcement of the Anti-Spoofing Provision. However well-intentioned the South Carolina Legislature and the governor may have been in passing the Act and signing it into the legislation, the Anti-Spoofing Provision overreaches. The Court should therefore strike down the Anti-Spoofing Provision just as other Federal Courts have done to similar overreaching statutes. *See, e.g., SpoofCard, LLC v. Burgum*, 2020 WL 7234159 (D.N.D. Nov. 9, 2020) (finding North Dakota's Anti-Spoofing Act to be unconstitutional); *TelTech Systems, Inc. v. Barbour*, 866 F.Supp.2d 571 (S.D. Miss. 2011) (finding Mississippi's "Caller ID Anti-Spoofing

Act" to be unconstitutional) *aff'd on other grounds sub nom. TelTech Systems, Inc. v. Bryant*, 702 F.3d 232 (5th Cir. 2012) (finding Mississippi's "Caller ID Anti-Spoofing Act to be conflict preempted by the Truth in Caller ID Act of 2009, codified at 47 U.S.C. § 227(e), and therefore not reaching the question of the Mississippi's statute's constitutionality); and *TelTech Systems, Inc. v. McCollum*, 2009 WL 10626585 (S.D. Fla. July 16, 2009) (finding Florida's "Caller ID Anti-Spoofing Act" to be unconstitutional).

II. PARTIES, JURISDICTION, AND VENUE

6. Plaintiff United Resource Systems, Inc. ("Plaintiff" or "URS") is a corporation organized and existing under the laws of the State of Colorado, with its principal place of business located in Colorado. Plaintiff is authorized to do business in South Carolina and its registered agent in South Carolina is Cogency Global Inc. located at 2 Office Park Court, Suite 103, Columbia, SC 29223.

7. Defendant Alan Wilson ("Wilson," the "Attorney General," or "Defendant") is the Attorney General of the State of South Carolina and is being sued in his official capacity as the proper individual on behalf of the State of South Carolina.

8. This Court has subject matter jurisdiction over the action and personal jurisdiction over the Defendant, and venue is proper in this district.

9. This case arises under the United States Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the federal Constitution and pursuant to 28 U.S.C. § 1331.

10. Personal jurisdiction exists over Defendant under Federal Rule of Civil Procedure 4(k)(1)(A) and South Carolina Rule of Civil Procedure 4(f).

11. Venue is proper in this district under 28 U.S.C. § 1391.

12. Injunctive relief is available as a remedy under Fed. R. Civ. Proc. 65.

III. FACTS APPLICABLE TO ALL CLAIMS

A. Nature of Caller ID Spoofing

13. Caller ID is a communications service that transmits to a called party the number from which a telephone call is apparently being made. The information is transmitted to the called party's telephone equipment before the call is answered. The caller ID information is usually displayed on the called party's telephone or on a separate but connected device. Depending on the sophistication of the called party's equipment, it may also provide to the called party a name associated with the caller ID. For example, a caller ID of 202-456-1414 should be associated with the name "White House" in a caller ID display.

14. A regular telephone call over the public switched telephone network (the "voice network" or "PSTN") is set up through the use of the Signaling System 7 ("SS7") out-of-band signaling system used by the landline (or "fixed line") telephone company switches to connect, maintain and bill for the call. The caller ID can be derived from the Automatic Number Identification ("ANI") or the Called Party Number ("CPN"), two of the SS7 data fields.

15. Many types of telephone equipment and software programs permit the caller to manipulate the caller ID by changing the CPN or, where there is no CPN, inserting data that SS7 reads as the CPN. For example, private branch exchanges ("PBXes") and other telephony hardware products made by dozens of manufacturers, including Nortel, Alcatel, Huawei, Lucent and Pingtel, all provide this capability. These products have been used for decades by millions of businesses. In addition, since 2000, several free open source software programs, including Asterisk, FreeSwitch, and SIPexchange, have been developed that provide equivalent PBX capability, including caller ID spoofing. These programs are free and can be run on any server or high-end personal or laptop computer.

16. Today a telephone call to someone on the PSTN need not be initiated from another telephone on the PSTN. In fact, a growing number of calls are made from other voice networks, such as mobile networks, or from the internet using a device based on Internet Protocol ("IP") technology, such as a computer, a smartphone, or an ATA (analog telephony adapter). On such an IP call, there is no PSTN number (and therefore no caller ID) associated with the caller or the device. Thus, many service providers input a default number that by definition "misleads" the called party about the identity of the caller. For example, unless a caller selected otherwise, Skype previously automatically inserted a default caller ID of 000123456 for all Skype-Out calls that originate in the U.S. (Skype-Out calls are calls from a device running Skype software to a number on the PSTN.) It appears that Skype's current default caller ID display is "No caller ID," "Unavailable," "Unknown," or something similar.

17. Many service providers offering IP to PSTN calling do not insert a uniform caller ID for all calls, as Skype did, but offer customers the capability of customizing their communication by allowing a customer to input a number and having that number transmitted by the IP network and read by the PSTN as a caller ID.

18. For example, SpoofCard LLC ("SpoofCard") is a company providing spoofing services. Its SpoofCard service is the most widely used caller ID spoofing service offered to consumers in the United States. The SpoofCard service operates like a regular long distance calling card service but also provides each customer the capability to alter (or "spoof") the caller ID that is displayed on a called party's telephone.

19. The process of using the SpoofCard service is essentially the same whether the customer is using a landline, a mobile phone or a computer to make a call. In each case, the customer will dial a local access number (also known as an inbound DID) to initiate the call. This

is the same for all calls, whether they are set up through a computer on the internet or within the mobile application.

20. The call is routed through the DID to a cloud-based communications provider from whom SpoofCard purchases inbound DID numbers and transport services. This inbound carrier converts the call from TDM format to internet protocol (IP) format if necessary (computer and some mobile phone calls are already in IP format), then transmits the call through a Session Initiation Protocol ("SIP") gateway and over its network to a cloud computing service (such as Google Cloud) where SpoofCard is running FreeSwitch, the soft switch program that SpoofCard uses.

21. When the call reaches the SpoofCard server, FreeSwitch runs a validation query on the phone number that the user wishes to display on their caller ID in order to ensure that it is a valid phone number and that it is not on SpoofCard's "do not spoof" list. If the number is validated, the requested change is made so that when the call is completed, it will appear to the receiving party's carrier that the call originated from the substituted caller ID. At the same time, SpoofCard checks the called number to ensure it does not appear on the SpoofCard Do Not Call list. For example, 911 centers and certain numbers for law enforcement agencies and financial services companies are on the list, so customers cannot make calls with spoofed caller ID to them.

22. The outbound call (still in IP format) is routed from the cloud computing servers over a different cloud-based communications provider network to the called party's network provider. Depending on their interconnection arrangements, either the transit provider or the called party's network converts the call to TDM format and thus bridges the calling phone with the receiving phone via the PTSN.

B. Nature of Trunk Line Calling

23. Trunk lines operate differently than call spoofing and do not involve the alteration of the number appearing on a caller ID. Instead, a caller acquires a bundle of local numbers within a state from a communications services provider, and from which the caller is able to make multiple outbound calls. A number from an area code in the state where the recipient's number originated is displayed on the caller ID of each recipient.

24. The displayed number on a call from a trunk line is an actual working telephone number belonging to the caller. Calls utilizing a trunk line can be made from locations outside the area code associated with the trunk line. For example, a party can obtain a trunk line for a number with an "803" area code, and place all calls on the trunk line from outside South Carolina. Any inbound call to the trunk line number, however, will go directly to the owner of the trunk line telephone number.

25. In its business, Plaintiff utilizes trunk lines with the area codes 803, 843, and 864, each of which is a "South Carolina area code" within the meaning of the term in the Anti-Spoofing Provision. Plaintiff obtains trunk line numbers from its communications services provider and has each bundle of telephone numbers for approximately 14 months, at which point its communications services provider assigns those numbers to different clients and provides Plaintiff with a new bundle of numbers for the state. Plaintiff is currently a defendant in a putative class action lawsuit filed the Richland County Court of Common Pleas, in which an individual is alleging that Plaintiff's use of a trunk line with an "843" area code violates the Anti-Spoofing Provision.

IV. THE FEDERAL LAW GOVERNING CALLER ID SPOOFING ON INTERSTATE CALLS

26. Until the enactment of the federal Truth in Caller ID Act of 2009, Public Law 111-331, 47 U.S.C. § 227(e), spoofing the caller ID on any interstate call was legal. In enacting the Truth in Caller ID Act, Congress specifically decided that caller ID spoofing should remain legal on interstate calls unless the calls are made with intent to "defraud, cause harm, or wrongfully obtain anything of value."

27. The legislative history of the Truth in Caller ID Act demonstrates beyond doubt that Congress intended that spoofed calls that were not made with the intent to "defraud, cause harm, or wrongfully obtain anything of value" were to remain legal. *TelTech Systems, Inc. v. Bryant,* 702 F.3d 232, 237 (5th Cir. 2012).

28. The legislative history of the Truth in Caller ID Act also demonstrates that it is intended to prohibit the manipulation of caller ID information under certain circumstances.

29. Congress also expressly excepted the blocking of caller ID information under the Truth in Caller ID Act. *See* 47 U.S.C. § 227(e)(2) ("Nothing in this subsection may be construed to prevent any person from blocking the capability of any caller identification service to transmit caller identification information.").

V. THE S.C. ANTI-SPOOFING PROVISION

30. The Anti-Spoofing Provision makes it illegal for a person to "make, place or initiate a call or text message or engage in conduct that results in the display of misleading, false or inaccurate caller identification information on the receiving party's telephone" "with the intent to defraud, harass, cause harm or wrongfully obtain anything of value…" *See* S.C. Code. Ann. § 37-21-50(A) (2018). The Anti-Spoofing Provision also makes it illegal for a person to "otherwise circumvent caller identification technology that allows the receiving party to identify from what

phone number, location, or organization the call or text message has originated from or misrepresent the origin and nature of the call or text message." *Id.*

31. Landline and wireless communications providers are excepted from the Anti-Spoofing Provision, unless the provider provides substantial assistance "when the provider knows or consciously avoids knowing such telephone solicitor is engaged in any act or practice that violates [the Anti-Spoofing Provision]." *See* S.C. Code Ann. § 37-21-50(B). Law enforcement agencies are also excepted, as are individuals engaging in such activity pursuant to a court order. *See* S.C. Code Ann. § 37-21-50(D).

32. A person who is alleged to have violated the Anti-Spoofing Provision is subject to a civil suit:

> (A) A person who is aggrieved by a violation of this chapter is entitled to initiate an action to enjoin the violation and to recover actual losses in addition to damages in the amount of one thousand dollars for each violation.
>
> (B) If the court finds a willful violation, the court may, in its discretion, increase the amount of the award to an amount not exceeding five thousand dollars for each violation.
>
> (C) Notwithstanding another provision of law, in addition to any damages awarded, the person initiating the action for a violation of this chapter may be awarded reasonable attorneys' fees and costs.
>
> (D) An action for damages, attorneys' fees, and costs brought pursuant to this section may be filed in an appropriate circuit court or municipal or magistrates court so long as the amount claimed does not exceed the jurisdictional limits as applicable. An action brought pursuant to this section that includes a request for an injunction must be filed in an appropriate circuit court.
>
> (E) It must be a defense to any action brought under this section that the violation was not intentional and resulted from a bona fide error.

S.C. Code Ann. § 37-21-80 (2018).

33. A person alleged to have violated the Anti-Spoofing Provision is also subject to administrative orders, an investigation by the Attorney General, and civil penalties:

> (A) The administrator, upon finding a violation of this chapter, may issue an administrative order requiring the person to cease and desist, to return property or money received in violation of this chapter and to impose penalties of up to five thousand dollars for each violation. The department may bring a civil action seeking similar relief, including injunctive relief, pursuant to subsection (B). Monies received in enforcement of this chapter shall be retained by the department for administration of this title.
>
> (B) (1) The Attorney General may investigate and enforce violations of this chapter. The Attorney General, may bring an action to enjoin a violation of this chapter by any person to recover damages for an aggrieved person or persons in the amount of five thousand dollars for each violation.
>
> (2) If the court finds a willful violation, the court, in its discretion, also may award a civil penalty of not more than five thousand dollars for each violation. Civil penalties awarded pursuant to this section in an action brought in the name of the State by the Attorney General must be paid to the general fund.
>
> (3) In an action brought pursuant to this section, the Attorney general may recover reasonable expenses incurred by the State or local governmental agency or department in investigating and preparing the case, and attorneys' fees.

S.C. Code Ann. § 37-21-90 (2018).

34. The plain language of the Anti-Spoofing Provision prohibits any use of caller ID spoofing so long as the caller has the requisite intent. The plain language of the Anti-Spoofing Provision also prohibits the use of caller ID spoofing, trunk lines, and blocking of a caller ID where it would prevent the receiving party from identifying from what phone number, location, or organization the call has originated. Since the plain language of the Anti-Spoofing Provision covers instances where the caller ID information prevents the receiving party from identifying the calling party's location, it also applies to individuals with South Carolina cell phone numbers who are travelling outside of South Carolina or who subsequently move outside South Carolina but retain their telephone number. Because there is no geographic limitation, the Anti-Spoofing Provision by definition covers interstate calls, where one party to the call is located outside of South Carolina.

35. The Anti-Spoofing Provision also specifically restricts the use of spoofing technology and trunk lines by callers located outside of South Carolina, thereby directly regulating interstate calls.

VI. THE EFFECT OF THE ANTI-SPOOFING PROVISION

36. Any person or company who uses spoofing, trunk lines, and/or caller ID blocking technology is subject to statutory liability of up to $5,000 for each call and a civil penalty of up to $5,000 for each call, as well as the costs for bringing any civil action against the person or company making the call.

37. The only exceptions to this liability are for "provider[s] of landline or wireless communications services merely by virtue of its involvement in delivering a call or text message initiated by or on behalf of a third party, unless the provider provides substantial assistance or support to the telephone solicitor initiating the call when the provider knows or consciously avoids knowing such telephone solicitor is engaged in any act or practice that violates this chapter[,]" law enforcement, and those engaged in the activity pursuant to a court order authorizing the use of caller identification manipulation.

38. Plaintiff does not qualify for any of these exceptions. Therefore, since the intent element does not appear to modify the provision regarding a caller who "otherwise circumvent[s] caller identification technology[,]" Plaintiff has potential liability under the Anti-Spoofing Provision for its use of trunk lines despite the fact that the trunk lines are valid telephone numbers belonging to Plaintiff and which, when called, are answered by Plaintiff. Moreover, even if the intent element applies to that provision, the impermissible expansion of the intent element beyond that found in the Truth in Caller ID Act puts Plaintiff at risk of incurring substantial costs defending itself in lawsuits despite lacking such intent, as evidenced by Plaintiff currently defending a purported class action in state court.

39. It is impossible for any user of caller ID spoofing, trunk lines, or caller ID blocking to ensure it is complying with the Anti-Spoofing Provision no matter how hard it tries. In order to be sure it is complying, a caller must know where the called party is located. Once upon a time when all telephones were landline phones connected to wall jacks, determining where calls began and ended was easy. This is unquestionably no longer true.

40. Given the present state of communications technology, neither a communications service provider nor any customer using caller ID spoofing, trunk lines, or caller ID blocking, can be sure anymore where a party receiving a call is actually located.

41. In addition, many communications service providers, particularly VoIP providers, mobile carriers, and calling card companies, also may not know where their own customers are located when they make or originate a call.

42. The reason that neither a caller using spoofing, trunk lines, or caller ID blocking technology, nor a communications service provider can be sure any more where a called party is actually located (or, in some cases, even where a call originates) is that four technological and regulatory developments in recent years have de-coupled the century-old link between the telephone number and the geographic location of the telephone user. These are (1) the tremendous growth of mobile phone usage (and its substitution for fixed or landline PSTN phone service), (2) the introduction of IP-based services, including VoIP, that interconnect with the old PSTN, (3) the imposition of number portability by the Federal Communications Commission ("FCC"), and (4) the growth of call forwarding service on landline telephones.

43. The tremendous growth in mobile phone usage is well documented. As the FCC and the courts recognize, many people, for business or personal reasons, have a mobile number that is associated with an area code other than the one where they live or work. Moreover, even

many people who live in the state associated with their mobile phone area code are making a substantial percentage of their calls from outside that state.

44. Similarly, there is no way to tell where many VoIP users are when they place a call or whether the call being placed is an interstate or intrastate call. A user of nomadic or mobile VoIP service can initiate or receive a call from anywhere in the world that he or she can find a broadband connection. Thus, there is no longer any automatic connection between the area code of a calling or called party's number and the party's location.

45. The effect of the growth of mobile and VoIP services has been exacerbated by the FCC's implementation of number portability, which gives a customer the right and the ability to take (or "port") his or her existing number when moving from one carrier to another *or one state to another*. Such porting is becoming more common, and many people are giving up their fixed landline service entirely and porting their fixed number to a VoIP or mobile carrier. Thus, every day a smaller percentage of total telephone calls are to or from fixed landline phones, the only phones whose location can ordinarily be expected to be within the geographic confines of the associated area code.

46. But even landlines are no longer tied to a geographic location, because there has been tremendous growth in call forwarding services. Such services are offered by landline telephone companies for free as part of their business packages and for free or as part of a bundled "unified communications" or "follow me" package by many new competitors (e.g., 8 x 8 (see https://www.8x8.com/unified-communications/ucaas) or Google Voice (see http://www.google.com/voice)). With the confluence of number portability and call forwarding, even a substantial percentage of calls that appear to be to landline phones in a specific area code are in fact terminated at phones outside the state to which that area code is assigned.

47. Given all these developments, it is not possible for a caller or service provider to know for certain where a called party is located. It may not even be possible in many cases for the service provider to know where the calling party - its own customer - is located.

48. It is possible for software technology used in providing telecom services to block calls to or from specific area codes, including those in which the numbers generally correspond to geographic locations in South Carolina. However, any attempt to block such calls would be both over-inclusive (because it would include calls made by or to mobile users and nomadic VoIP subscribers with South Carolina area code numbers but who are actually located outside of South Carolina) and under-inclusive (because it would not include calls made by or to mobile users or nomadic VoIP subscribers with non-South Carolina area code numbers but who are actually located in South Carolina when the calls are made). Therefore, blocking calls to South Carolina area codes cannot ensure that no calls to or from South Carolina use caller ID spoofing services. Moreover, such blocking would prevent users in other states from using services which are legal in those states.

49. On its face, the Anti-Spoofing Provision also prohibits various forms of constitutionally protected speech, including anonymous speech, pseudonymous speech, and the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy.

COUNT I
CONFLICT WITH AND PREEMPTION BY GOVERNING FEDERAL LAW

50. Plaintiff restates and incorporates by reference each and every allegation in the preceding paragraphs as if fully set forth herein.

51. The Anti-Spoofing Provision violates the Supremacy Clause (Article VI, Clause 2) of the United States Constitution, which provides that "[t]his Constitution, and the Laws of the

United States which shall be made in Pursuance thereof; . . . shall be the supreme Law of the land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding."

52. The Anti-Spoofing Provision conflicts in substantial part with, and therefore is preempted by, 47 U.S.C. § 227(e), part of the federal Truth in Caller ID Act of 2009. The conflict lies in the fact that Congress specifically decided that caller ID spoofing should be legal on interstate calls unless the calls are made with intent to "defraud, cause harm, or wrongfully obtain anything of value," while the Anti-Spoofing Provision makes a wide array of such calls illegal in interstate commerce involving South Carolina. Congress further elected not to restrict the use of trunk lines and specifically stated that the Truth in Caller ID Act does not prohibit the use of caller ID blocking technology. The conflict between the federal and state laws prevents the achievement of the Congressional purpose underlying the enactment of the Truth in Caller ID Act of 2009.

COUNT II
VIOLATION OF THE INTERSTATE COMMERCE CLAUSE

53. Plaintiff restates and incorporates by reference each and every allegation in the preceding paragraphs as if fully set forth herein.

54. The Anti-Spoofing Provision effectively prohibits the spoofing of caller ID on interstate telephone calls. It further prohibits non-spoofed calls where the caller has a valid number with a South Carolina area code but is placing the call from outside South Carolina, as well as the use of caller ID blocking technology. Moreover, subsection (1) of the Anti-Spoofing Provision specifically regulates interstate calls.

55. The Anti-Spoofing Provision is unconstitutional because it violates the Interstate Commerce Clause (Article I, Section 8, Clauses 1 and 3) of the United States Constitution, which

provides that "[t]he Congress shall have power . . . [t]o regulate commerce with foreign nations, and among the several states, and with the Indian tribes; . . ."

56. The Constitution and laws of the United States preempt the ability of the State of South Carolina to regulate the spoofing of caller ID on interstate telephone calls, to regulate the use of numbers with South Carolina area codes by persons located outside South Carolina, and to regulate the use of caller ID blocking technology.

COUNT III
VIOLATION OF THE DORMANT COMMERCE CLAUSE

57. Plaintiff restates and incorporates by reference each and every allegation in the preceding paragraphs as if fully set forth herein.

58. The Anti-Spoofing Provision violates the dormant Commerce Clause of the United States Constitution because it will inevitably have an impermissible effect on interstate commerce conducted wholly outside the State of South Carolina.

COUNT IV
VIOLATION OF THE FIRST AND FIFTH AMENDMENT
RIGHT TO FREE SPEECH – OVERBREADTH AND VAGUENESS

59. Plaintiff restates and incorporates by reference each and every allegation in the preceding paragraphs as if fully set forth herein.

60. The First Amendment to the United States Constitution provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." The Fifth Amendment provides that "[n]o person shall . . . be deprived of life, liberty, or property, without due process of law . . ."

61. The Anti-Spoofing Provision violates the First and Fifth Amendments because it is substantially overbroad.

62. The Anti-Spoofing Provision violates the First and Fifth Amendments because it is not the least restrictive means of accomplishing any compelling governmental purpose.

COUNT V
VIOLATION OF THE FIRST, FIFTH AND FOURTEENTH AMENDMENT RIGHT TO COMMUNICATE

63. Plaintiff restates and incorporates by reference each and every allegation in the preceding paragraphs as if fully set forth herein.

64. Section 1 of the Fourteenth Amendment prohibits a state from trampling any of the First or Fifth Amendment freedoms. It provides in relevant part that "[n]o State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

65. The Anti-Spoofing Provision is unconstitutional because it violates the First, Fifth and Fourteenth Amendments by denying citizens their right to communicate anonymously and pseudonymously.

COUNT VI
DECLARATORY JUDGMENT

66. Plaintiff restates and incorporates by reference each and every allegation in the preceding paragraphs as if fully set forth herein.

67. There is a real and actual controversy between Plaintiff and Defendant regarding whether the Anti-Spoofing Provision is preempted by federal law or is unconstitutional.

68. Plaintiffs seek a Declaratory Judgment pursuant to 28 U.S.C § 2201 and Fed. R. Civ. Proc. 57 for the purpose of determining and adjudicating questions of actual controversy between the parties.

69. Plaintiffs contend that the Anti-Spoofing Provision:

a. Conflicts with and is therefore preempted by federal law;

b. Is unconstitutional because it violates the Interstate Commerce Clause of the United States Constitution; and

c. Is unconstitutional because it violates the First, Fifth and Fourteenth Amendments to the United States Constitution.

70. Plaintiff is informed, believes, and alleges that Defendant contend the contrary of each of (a), (b) and (c).

71. Wherefore the Plaintiff requests that the Court determine and adjudge that each of the propositions in Paragraph 69 is correct, and that the Anti-Spoofing Provision is both preempted by federal law and unconstitutional, and for each reason is therefore unenforceable.

COUNT VII
VIOLATION OF THE CIVIL RIGHTS ACT (42 U.S.C. § 1983)

72. Plaintiff restates and incorporates by reference each and every allegation in the preceding paragraphs as if fully set forth herein, and further allege as follows:

73. Defendant is an individual who, under color of statute, ordinance, regulation, custom, or usage, of the State of South Carolina, is subjecting, or causing to be subjected, said Plaintiff to the deprivation of rights, privileges, or immunities secured by the Constitution and laws of the United States—specifically, the Supremacy and Commerce Clauses of the United States Constitution.

74. Defendant's conduct violates 42 U.S.C. § 1983.

75. Without relief from this Court, Defendant, acting under color of statute, ordinance, regulation, custom, or usage of the State of South Carolina, will continue to subject, or cause to be subjected, the Plaintiff to the deprivation of rights, privileges, or immunities secured by the Constitution and laws of the United States.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for itself and all others similarly situated that the Court enter an order:

1. Assuming jurisdiction of this action;

2. Declaring that the Anti-Spoofing Provision is preempted by federal law and violates the Constitution and laws of the United States;

3. Enjoining Defendant, his agents, servants, employees, successors and assigns, and all others in concert or in privity with them, from bringing or threatening to bring any civil enforcement action, or from otherwise attempting to enforce, the Anti-Spoofing Provision;

4. Awarding damages to Plaintiff in an amount equal to damages proven at trial;

5. Awarding the Plaintiff its reasonable attorney's fees and costs pursuant to 42 U.S.C. § 1988; and

6. Granting Plaintiff such further relief as the Court may deem just and equitable.

Dated: February 4, 2021.

Respectfully submitted by:

/s/ Chad V. Echols
Chad V. Echols (Fed I.D. 9810)
David A. Grassi, Jr. (Fed I.D. 12963)
The Echols Firm, LLC
PO Box 12645
Rock Hill, SC 29731
Phone: (803) 329-8970
Email: chad.echols@theecholsfirm.com
Email: david.grassi@theecholsfirm.com

ATTORNEYS FOR PLAINTIFF
UNITED RESOURCE SYSTEMS, INC.